Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 301 (2005) 89–105

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

PD-sets for the codes related to some classical varieties

Hans-Joachim Kroll, Rita Vincenti

Zentrum Mathematik Technische Universität München, Germany, Dipartimento di Matematica e Informatica, Universita' degli Studi, Perugia, Italy

Received 31 July 2002; received in revised form 6 May 2004; accepted 8 November 2004
Available online 2 September 2005

Abstract

We generalize the notion of a PD-set of a code to that of a t-PD-set of an arbitrary permutation set. We find PD-sets for miquelian Benz planes of small order and for the ruled rational normal surface of order 3 in PG(4, 3) and in PG(4, 4). These results yield PD-sets for the related linear codes.

Keywords: Linear code; Projective system; PD-set; Variety

1. Introduction

Permutation decoding is a technique developed in 1964 by F.J. MacWilliams and uses a subset of the automorphism group of the code to assist in decoding a received vector. Results were added by Mitchell and Rudolph (1964), Gordon (1982), Key (2001) and other authors (cf. [8]). A PD-set for a t-error-correcting code C is a set S of automorphisms of the code which is such that every possible error vector of weight t or less can be moved by some member of S out of the information positions. Concerning the question of how to apply a PD-set to decode a message we refer the reader to Huffman's article "Codes and groups" in [8, pp. 1345–1440], where an algorithm is given. The permutation decoding algorithm is more efficient the smaller the size of the PD-set. A lower bound on this size is given in [3] (cf. [8, p. 1414]).

E-mail addresses: kroll@ma.tum.de (H.-J. Kroll), alice@unipg.it (R. Vincenti).

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.11.020

When a code has a large automorphism group it is likely that a PD-set can be found. Large automorphism groups can be expected for linear codes defined by projective systems. In Section 2 we describe how the automorphisms fixing a subset of points P in a finite projective space induce automorphisms of the code defined by the projective system P (cf. Proposition 2). Also, we generalize the notion of a PD-set of a code to that of a t-PD-set of an arbitrary permutation set.

In Section 3 we are concerned with codes related to quadrics in three-dimensional finite projective spaces $\mathrm{PG}(3, q)$. Since the geometries of the plane sections of an elliptic or hyperbolic quadric or a cone over a conic are miquelian Benz planes, the automorphism groups of these quadrics are known. For all three cases we present PD-sets for $q = 3$ (cf. Proposition 6, 8, 9). For the elliptic and hyperbolic quadric we give also examples for $q = 4$ (cf. Proposition 7, 10). These results say that the corresponding codes admit PD-sets S. The size $|S|$ is in some cases minimal.

In the last section we consider codes related to what we call the *celtic variety* P, i.e., the ruled rational normal surface of order 3 in the four-dimensional projective space $\mathrm{PG}(4, q)$. After presenting an automorphism group (cf. Proposition 14) we give examples of PD-sets of P for $q = 3$ and $q = 4$ (cf. Proposition 16, 18).

2. Automorphisms of a code defined by a projective system

For the convenience of the reader, and in order to establish our notations we will recall the basic definitions.

Let $K = \mathrm{GF}(q)$ be the Galois field of order q and $K^* = K\backslash\{0\}$. For $n \in \mathbb{N}$, a *linear code C of length n* is a vector subspace of the vector space K^n. For $\mathbf{x} \in K^n$ the set $\mathrm{supp}(\mathbf{x}) = \{i \in \mathbb{N} \mid i \leqslant n, x_i \neq 0\}$ is the support of $\mathbf{x}$, and $\mathrm{wt}(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})|$ is the weight of $\mathbf{x}$.

A linear code C of length n is an $[n, k, d]_q$*-code* if $k = \dim\ C$ is the dimension of C and $d = \min\{\mathrm{wt}(\mathbf{c}) \mid \mathbf{c} \in C, \mathbf{c} \neq 0\}$ is the minimum weight of C.

Let (V, K) be a k-dimensional vector space over K and, for $s \in \mathbb{N}$ with $s \leqslant k - 1$, let $\mathfrak{S}_s$ be the set of all s-dimensional vector subspaces of (V, K). We denote by $\hat{V}$ the dual vector space of V, i.e., the vector space of all linear forms $f : V \to K$.

Let $V_0 = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset V$ be a subset of V with n elements. Then V_0 is called an $[n, k, d]_q$*-system*, if the linear hull of V_0 is V and if

$$d = n - \max\{|V_0 \cap H| \,|\, H \in \mathfrak{S}_{k-1}\}.$$

.

Proposition 1 (*cf. Tsfasman [9, p. 10]*). *Let $V_0 = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be an $[n, k, d]_q$-system of the vector space (V, K) and* $\mathrm{Ev} : \hat{V} \to K^n$, $f \mapsto c_f = (f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$. *Then the image $C(V_0) = \mathrm{Ev}(\hat{V})$ is an $[n, k, d]_q$-linear code.*

For $\mathbf{x} \in V^* = V\backslash\{0\}$, denote $K^*\mathbf{x} = \{\lambda\mathbf{x} \mid \lambda \in K^*\}$, and $V^*/K^* = \{K^*\mathbf{x} \mid \mathbf{x} \in V^*\}$. Let $\varphi : V^* \to V^*/K^*$, $\mathbf{x} \mapsto K^*\mathbf{x}$ be the canonical map.

Let $\mathrm{PG}(k - 1, q)$ denote the $(k - 1)$-dimensional projective space over K, i.e., V^*/K^* is the set of points and $\mathfrak{L} = \{\varphi(L^*) \mid L \in \mathfrak{S}_2\}$ is the set of lines. A map $\mathbf{v} : V^*/K^* \to V^*$, $p \mapsto \mathbf{v}(p)$ is a *vector representation* if, for every $p \in V^*/K^*$, we have $p = K^*\mathbf{v}(p)$.

For $M \subset V^*/K^*$ the hull $\overline{M}$ is the smallest subspace of $\mathrm{PG}(k-1,q)$ containing M (cf. [7]). Let $\mathfrak{H}$ denote the set of all hyperplanes of the projective space $\mathrm{PG}(k-1,q)$. Let $P=\{p_1,\ldots,p_n\} \subset V^*/K^*$ be an n-set of points of $\mathrm{PG}(k-1,q)$. Then P is an $[n,k,d]_q$-*projective system* if the hull $\overline{P}=V^*/K^*$ and $d=n-\max\{|P\cap H||H\in\mathfrak{H}\}$. Here, P is an $[n,k,d]_q$-projective system if and only if $\mathbf{v}(P)$ is an $[n,k,d]_q$-system of V.

Denote by $C(\mathbf{v},P)=C(\mathbf{v}(P))$ the $[n,k,d]_q$-linear code defined in Proposition 1 by the $[n,k,d]_q$-system $\mathbf{v}(P)$. If $\mathbf{v}_1$, $\mathbf{v}_2 : V^*/K^* \to V^*$ are two vector representations then the codes $C(\mathbf{v}_1,P)$ and $C(\mathbf{v}_2,P)$ are isomorphic because, for $f\in\hat{V}$ and $x\in P$, we have $f(\mathbf{v}_1(x))=0$ if and only if $f(\mathbf{v}_2(x))=0$, hence $\mathrm{wt}(f\mathbf{v}_1(p_1),\ldots,f\mathbf{v}_1(p_n)) = \mathrm{wt}(f\mathbf{v}_2(p_1),\ldots,f\mathbf{v}_2(p_n))$.

We call a collineation $\alpha := V^*/K^* \to V^*/K^*$ *projective* if α is induced by a linear bijection $\tilde{\alpha}: V\to V$, i.e. $\alpha(p)=K^*\tilde{\alpha}(\mathbf{v}(p))$.

Let $P=\{p_1,\ldots,p_n\}\subset V^*/K^*$ be an $[n,k,d]_q$-projective system, and let $\mathrm{Aut}\,P$ denote the group of all projective collineations α with $\alpha(P)=P$.

For $\alpha\in\mathrm{Aut}\,P$ there is exactly one permutation $\sigma_\alpha\in \mathrm{S}_n$ with $p_{\sigma_\alpha(i)}=\alpha^{-1}(p_i)$. Let $\tilde{\alpha}: V\to V$ be a linear bijection inducing α. Then there are $d_1,\ldots,d_n\in K^*$ with $d_i\mathbf{v}(\alpha(p_i))=\tilde{\alpha}(\mathbf{v}(p_i))$. Put $\mathbf{d}_{\tilde{\alpha}}=(d_1,\ldots,d_n)$.

Every permutation $\sigma\in\mathrm{S}_n$ induces a linear bijection

$$\tilde{\sigma}: K^n\to K^n,\quad \mathbf{x}=(x_1,\ldots,x_n)\mapsto \mathbf{x}\sigma=(x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(n)})$$

and every $\mathbf{d}=(d_1,\ldots,d_n)\in(K^*)^n$ induces a linear bijection

$$\tilde{\mathbf{d}}: K^n\to K^n,\quad \mathbf{x}=(x_1,\ldots,x_n)\mapsto \mathbf{x}\mathbf{d}=(x_1d_1,\ldots,x_nd_n).$$

The linear bijection $(\mathbf{d};\sigma)=\tilde{\sigma}\circ\tilde{\mathbf{d}}$, $\mathbf{x}\mapsto(\mathbf{x}\mathbf{d})\sigma$ is called a *monomial bijection* (cf. [4, p. 202], [8, p. 1348]). Every monomial bijection is weight preserving.

Now let us return to the linear bijection $\tilde{\alpha}: V\to V$ inducing the collineation α. Since $\tilde{\alpha}_r : \hat{V}\to\hat{V}$, $f\mapsto f\circ\tilde{\alpha}$ is a linear bijection the mapping $\overline{\alpha}: C(\mathbf{v},P)\to C(\mathbf{v},P)$, $\mathbf{c}_f\mapsto\mathbf{c}_{f\circ\tilde{\alpha}}$ is a linear bijection. For $f\in\hat{V}$ we have

$$\overline{\alpha}(\mathbf{c}_f)=(f\tilde{\alpha}(\mathbf{v}(p_i)))=(f(d_i\mathbf{v}(\alpha(p_i))))=(d_i f(\mathbf{v}(p_{\sigma_\alpha^{-1}(i)})))=(\mathbf{d}_{\tilde{\alpha}};\sigma_\alpha)(\mathbf{c}_f);$$

i.e., $\overline{\alpha}$ is a monomial automorphism of the linear code $C(\mathbf{v},P)$ with *diagonal part* $\mathbf{d}_{\tilde{\alpha}}$ and *permutation part* σ_α (cf. [8, p. 1350]).

Let $\mathrm{MAut}\,C(\mathbf{v},P)$ and $\mathrm{MAut}_{pr}C(\mathbf{v},P)$ denote the groups of all monomial automorphisms of $C(\mathbf{v},P)$ and of all permutation parts of the monomial automorphisms of $C(\mathbf{v},P)$.

Proposition 2. *Let $P=\{p_1,\ldots,p_n\}$ be an $[n,k,d]_q$-projective system. Denote $\tilde{}$:$\mathrm{Aut}\,P\to\mathrm{GL}(k,q)$, $\alpha\mapsto\tilde{\alpha}$ a mapping such that $\tilde{\alpha}$ induces α. Then the mapping*

$$\Phi:\begin{cases}\mathrm{Aut}\,P\to\mathrm{MAut}\,C(\mathbf{v},P)\\ \alpha\mapsto(\mathbf{d}_{\tilde{\alpha}};\sigma_\alpha)\end{cases}$$

is injective and the mapping

$$\Psi:\begin{cases}\mathrm{Aut}\,P\to\mathrm{MAut}_{pr}C(\mathbf{v},P)\\ \alpha\mapsto\sigma_\alpha\end{cases}$$

is an antimonomorphism.

Proof. Let $\alpha, \beta \in \mathrm{Aut}\, P$. For $\alpha \neq \beta$ we have $\alpha^{-1} \neq \beta^{-1}$, thus there is an $i \in \{1, \ldots, n\}$ with $\alpha^{-1}(p_i) \neq \beta^{-1}(p_i)$, and hence $\sigma_\alpha(i) \neq \sigma_\beta(i)$. Therefore Ψ and Φ are injective. Also,

$$p_{\sigma_{\beta\alpha}(i)} = (\beta\alpha)^{-1}(p_i) = \alpha^{-1}\beta^{-1}(p_i) = \alpha^{-1}(p_{\sigma_\beta(i)}) = p_{\sigma_\alpha\sigma_\beta(i)};$$

hence $\Psi(\beta \circ \alpha) = \Psi(\alpha)\Psi(\beta)$. □

Let C be an $[n, k, d]_q$-linear t-error-correcting code, $I \subset \{1, \ldots, n\}$ a set of information positions and $S \subset \mathrm{MAut}\, C$. Then S is called a *permutation decoding set*, a PD-set for short, if for every subset $B \subset \{1, \ldots, n\}$ with $|B| \leqslant t$ there exists an automorphism in S with permutation part σ s.t. $\sigma(B) \cap I = \emptyset$. (cf. [8, p. 1413]). A lower bound for a PD-set S is given in the next result.

Theorem 3 (*Gordon [3], cf. [8]*). *Let S be a* PD*-set for a t-error-correcting $[n, k]$-code with redundancy $r = n - k$. Then*

$$|S| \geqslant \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil.$$

Let $P = \{p_1, \ldots, p_n\}$ be an $[n, k, d]_q$-projective system, $I \subset \{1, \ldots, n\}$ with $|I| = k$ and $P_I = \{p_i \mid i \in I\}$. Then I is a set of information positions of $C(\mathbf{v}, P)$ if and only if P_I is a set of independent points of the projective space $\mathrm{PG}(k-1, q)$. Let P_I be an independent k-set and $\Sigma \subset \mathrm{Aut}\, P$. Then Σ is a PD-*set with respect to* P_I if for every subset $B \subset P$ with $|B| \leqslant \lfloor (d-1)/2 \rfloor$ there is an automorphism $\alpha \in \Sigma$ with $\alpha(B) \subset P \setminus P_I$.

By Proposition 2 the set Σ is a PD-set for (P, P_I) if and only if $S = \Phi(\Sigma)$ is a PD-set for the code $C(\mathbf{v}, P)$. Therefore the problem to find a PD-set for the code $C(\mathbf{v}, P)$ is reduced to the problem to find a PD-set for (P, P_I). If the automorphism group $\mathrm{Aut}\, P$ is large it might be promising to find a PD-set Σ in $\mathrm{Aut}\, P$ or equivalently in any isomorphic permutation group. In this context we generalize the notion of a PD-set for any permutation group (P, Γ), where Γ is a subgroup of the symmetric group on the set P. Let $I \subset P$, $t \in \mathbb{N}$ and $\Sigma \subset \Gamma$. Then Σ is called a t-PD-*set* for I, if for every subset $B \subset P$ with $|B| \leqslant t$ there is a $\sigma \in \Sigma$ with $\sigma(B) \subset P \setminus I$.

Remark. If Σ is a t-PD-set for $I \subset P$ and $\alpha \in \mathrm{Aut}\, P$, then $\alpha\Sigma$ is a t-PD-set for $\alpha(I)$. If $\alpha^{-1} \in \Sigma$ then the t-PD-set $\alpha\Sigma$ contains the identity.

Proposition 4. *Let P be an $[n, k, d]_q$-projective system of* $\mathrm{PG}(k-1, q)$*, let $I \subset P$, and let $\Sigma \subset \mathrm{Aut}\, P$ be a* PD*-set with respect to I. Also, let $D \subset P$ with $|D| \leqslant \lfloor (d-1)/2 \rfloor$ and $\alpha(D) = D$ for all $\alpha \in \Sigma$ such that $P_0 = P \setminus D$ generates* $\mathrm{PG}(k-1, q)$*. Then*
(1) *$D \cap I = \emptyset$;*
(2) *P_0 is an $[n_0, k, d_0]_q$-projective system with $n_0 = n - |D|$ and $d_0 \leqslant d$;*
(3) *Σ is a* PD*-set for the projective system P_0 with respect to I.*

Proof. (1) From $\alpha(D) = D$ for all $\alpha \in \Sigma$ and $D \cap I \neq \emptyset$ it follows that $\alpha(D) \cap I \neq \emptyset$ contradicting the assumption that Σ is a PD-set.

(2) Clearly, P_0 is a projective system with $n_0 = n - |D|$. For $H \in \mathfrak{H}$,

$H \cap P_0 = H \cap P \backslash H \cap D$. Hence

$|H \cap P_0| = |H \cap P| - |H \cap D| \geqslant |H \cap P| - |D|$;

thus $\max\{|H \cap P_0||H \in \mathfrak{H}\} \geqslant \max\{|H \cap P||H \in \mathfrak{H}\} - |D|$. Therefore,

$$d_0 = n_0 - \max\{|H \cap P_0||H \in \mathfrak{H}\} \leqslant n - \max\{|H \cap P||H \in \mathfrak{H}\} = d.$$

(3) By (1) we have $I \subset P_0$. Since $d_0 \leqslant d$ and Σ is a PD-set for P, the set Σ is a PD-set of P_0. □

3. Embedded Benz planes as projective systems and examples of PD-sets

Let Q be an elliptic quadric or a cone with vertex s over a conic or a hyperbolic quadric in the three-dimensional projective space $\mathrm{PG}(3, q)$ over the Galois field $K = \mathrm{GF}(q)$. Then (cf. [5, p. 4])

$$|Q| = \begin{cases} q^2 + 1 & \text{if } Q \text{ is elliptic,} \\ q(q+1) + 1 & \text{if } Q \text{ is a cone,} \\ (q+1)^2 & \text{if } Q \text{ is hyperbolic.} \end{cases} \tag{1}$$

Let $H \in \mathfrak{H}$ be a plane of $\mathrm{PG}(3, q)$. If Q is elliptic, then the intersection $Q \cap H$ is a point or a conic. If Q is a cone, then $Q \cap H$ is the vertex s or a line or the union of two lines or a conic. If Q is hyperbolic, then $Q \cap H$ is the union of two lines or a conic. Therefore,

$$\max\{|Q \cap H| \mid H \in \mathfrak{H}\} = \begin{cases} q+1 & \text{if } Q \text{ is elliptic,} \\ 2q+1 & \text{otherwise.} \end{cases} \tag{2}$$

Eqs. (1), (2) and Proposition 4, give the following result.

Proposition 5. (1) *If Q is elliptic, then $P = Q$ is a $[q^2+1, 4, q(q-1)]_q$-projective system.*
(2) *If Q is a cone, then $P = Q\backslash\{s\}$ is a $[q(q+1), 4, q(q-1)]_q$-projective system.*
(3) *If Q is hyperbolic, then $P = Q$ is a $[(q+1)^2, 4, q^2]_q$-projective system.*

As in Proposition 5 let $P = Q\backslash\{s\}$ if Q is a cone and $P = Q$ otherwise. For a plane $H \in \mathfrak{H}$ we call the plane section $Q \cap H$ non-trivial if $Q \cap H$ is a conic. Let $\mathfrak{C}$ denote the set of all non-trivial plane sections of Q. Then $(P, \mathfrak{C})$ is a miquelian Benz plane, i.e., a miquelian Möbius, Laguerre or Minkowski plane if Q is an elliptic quadric, a cone or a hyperbolic quadric, respectively.

The miquelian Benz planes can be represented as chain geometries $\Sigma(K, L)$ over the unitary K-algebras L of rank 2 (cf. [1]). In this context we need only the set of points $\mathbb{P}(L)$ of $\Sigma(K, L)$ and a subgroup of the automorphism group of $\Sigma(K, L)$. Let L^* denote the group of the units of L. The set of points of $\Sigma(K, L)$ is the projective line

$$\mathbb{P}(L) = \{L^*(x, y) | x, y \in L, \exists a, b \in L : xa + yb = 1\}.$$

The linear group $\mathrm{GL}(2, L)$ over L is the group of the (2×2)-matrices

$$\mathfrak{A} = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$$

with $a_{ij} \in L$ and $a_{11}a_{22} - a_{12}a_{21} \in L^*$. The projective linear group $\mathrm{PGL}(2, L)$ consists of the permutations γ of $\mathbb{P}(L)$ induced by the matrices $\mathfrak{A} \in \mathrm{GL}(2, L)$ as follows: $\gamma : L^*(x, y) \mapsto L^*(x, y)\mathfrak{A}$ (cf. [1]).

The group $\mathrm{PGL}(2, L)$ is a subgroup of the automorphism group of $\Sigma(K, L)$. Also, every automorphism τ of L with $K^\tau = K$ induces an automorphism $\alpha_\tau : \mathbb{P}(L) \to \mathbb{P}(L)$, $L^*(x, y) \mapsto L^*(x^\tau, y^\tau)$ of $\Sigma(K, L)$ (cf. [1, p. 99]).

Let $\mathscr{A}_0(L, K)$ denote the group of all automorphisms τ of L with $K \subset \mathrm{Fix}\,\tau$. If we identify the automorphisms $\tau \in \mathscr{A}_0(L, K)$ with the induced automorphisms α_τ of $\Sigma(K, L)$, the set $\mathbb{M}_K(K, L) = \mathrm{PGL}(2, L) \circ \mathscr{A}_0(L, K)$ is a subgroup of the automorphism group of $\Sigma(K, L)$. The product $\mathrm{PGL}(2, L) \circ \mathscr{A}_0(L, K)$ is faithful (cf. [1, p. 100]).

The algebras L of rank 2 over $K = \mathrm{GF}(q)$ are the quadratic field extension $\mathrm{GF}(q^2)$, the dual numbers $\mathbb{D} = K + K\varepsilon$ with $\varepsilon^2 = 0$ and the anormal complex numbers $\mathbb{A} = K \times K$ with componentwise addition and multiplication (cf. [1]). In each case there is an automorphism $^- : L \to L$ with $K \subset \mathrm{Fix}^-$ and $\overline{\overline{z}} = z$ for all $z \in L$, namely $z \mapsto z^q$, $x + y\varepsilon \mapsto x - y\varepsilon$, and $(x, y) \mapsto (y, x)$, respectively.

The chain geometry $\Sigma(K, L)$ is a Möbius, Laguerre and Minkowski plane, if $L = \mathrm{GF}(q^2)$, $L = \mathbb{D}$ and $L = \mathbb{A}$, respectively.

Let $V = K \times L \times K$ denote the direct sum of the vector spaces K, L, and K. Then

$$\mathscr{B} : \begin{cases} \mathbb{P}(L) \to V^*/K^* \\ L^*(x, y) \mapsto K^*(x\overline{x}, x\overline{y}, y\overline{y}) \end{cases}$$

is a well defined and injective mapping (cf. [6]). The image $\mathscr{B}(\mathbb{P}(L) = P$ consists of the regular points of the quadric $Q = \{K^*(x_0, z, x_3) \in V^*/K^* \mid z\overline{z} - x_0x_3 = 0\}$.

Also , for every $\alpha \in \mathbb{M}_K(K, L)$ the bijection $\mathscr{B}\alpha\mathscr{B}^{-1} : P \to P$ is an automorphism of P (cf. [6]). Hence

$$\mathscr{B}^* : \begin{cases} \mathbb{M}_K(K, L) \to \mathrm{Aut}\, P \\ \alpha \mapsto \mathscr{B}\alpha\mathscr{B}^{-1} \end{cases}$$

is a monomorphism. Since $\mathscr{B}$ and $\mathscr{B}^*$ are injective mappings, the following result is obtained.

Lemma 1. *Let L be a unitary algebra of rank 2 over the field K and Σ a* t-PD-*set for $I \subset \mathbb{P}(L)$ with $|I| = 4$. Then $\mathscr{B}^*(\Sigma)$ is a* PD-*set of the projective system $\mathscr{B}(\mathbb{P}(L))$ for $\mathscr{B}(I)$ if $\mathscr{B}(I)$ is an independent set of the projective space V^*/K^*.*

In the following, for an algebra L let us identify the element $x \in L$ with the point $L^*(x, 1)$ of the projective line $\mathbb{P}(L)$, and the point $L^*(1, 0)$ with ∞.

For $a \in L$ we denote by a^+ the *translation* induced by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$, and for $m \in L^*$ let $m^\bullet$ be the bijection induced by $\left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Also, denote by $\iota : \mathbb{P}(L) \to \mathbb{P}(L)$ the involution induced by the martix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

For $x \in L$ we have $a^+(x) = a^+(L^*(x,1)) = L^*(x+a,1) = x+a$, $m^\bullet(x) = xm$, and $a^+(\infty) = \infty = m^\bullet(\infty)$. For $x \in L^*$ we have $\imath(x) = L^*(1,x) = x^{-1}$ and $\imath(\infty) = 0$.

Proposition 6. *Let $K = \mathrm{GF}(3)$ and $L = \mathrm{GF}(3^2) = K(w)$ with $w^2 = 2$. Then*

$$\Sigma = \{\mathrm{id}, (1+2w)^+ 2^\bullet, \imath w^+ 2^\bullet, 2^+ \imath (2w)^\bullet 1^+\}$$

is a 2-PD*-set for $I = \{0,1,2,w\}$ and $\mathscr{B}(I)$ is an independent set of the projective space V^*/K^*. The lower bound for a* 2-PD*-set for I is* 4.

Proof. Put $\sigma_0 = \mathrm{id}$, $\sigma_1 = (1+2w)^+ 2^\bullet$, $\sigma_2 = \imath w^+ 2^\bullet$, $\sigma_3 = 2^+ \imath (2w)^\bullet 1^+$ and $A_i = \sigma_i^{-1}(I)$. Then

$$A_0 = \{0,1,2,w\}, \quad A_1 = \{1+2w, 2w, 2+2w, 1+w\},$$

$$A_2 = \{\infty, 2+w, 1+w, 2w\}, \quad A_3 = \{2+w, 2w+2, \infty, 2w+1\}.$$

Let $B = \{b_0, b_1\} \subset \overline{L} = L \cup \{\infty\}$. Then

$$\sigma_i(B) \subset \overline{L} \backslash I \iff B \subset \overline{L} \backslash A_i \iff B \cap A_i = \emptyset.$$

Let $B \cap A_i \neq \emptyset$ for $i = 0, 1, 2$. We may assume $b_0 \in A_0$. Since $A_0 \cap A_1 = \emptyset$, $A_0 \cap A_2 = \emptyset$ and $A_0 \cap A_3 = \emptyset$, so we have $b_0 \notin A_1, A_2, A_3$. Therefore $B \cap A_1 \neq \emptyset$, $B \cap A_2 \neq \emptyset$ and $b_0 \notin A_1, A_2$ implies $b_1 \in A_1 \cap A_2 = \{2w, 1+w\}$. Hence $b_0, b_1 \notin A_3$, i.e., $B \cap A_3 = \emptyset$, thus $\sigma_3(B) \subset \overline{L} \backslash I$.

The image of I under $\mathscr{B}$ is

$$\mathscr{B}(I) = \{K^*(0,0,1), K^*(1,1,1), K^*(1,2,1), K^*(1,w,1)\},$$

where the middle component is in the quadratic extension L. Since $(0,0,1)$, $(1,1,1)$, $(1,2,1)$, $(1,w,1)$ are linear independent $\mathscr{B}(I)$ is an independent set of V^*/K^*. By Theorem 3 we have $|\Sigma| \geqslant \left\lceil \frac{10}{6} \left\lceil \frac{9}{5} \right\rceil \right\rceil = 4$. $\square$

Proposition 7. *Let $K = \mathrm{GF}(4) = \mathbb{Z}_2(d)$ with $d^2 = d+1$ and $L = \mathrm{GF}(4^2) = K(w)$ with $w^2 = w+d$. Put $\sigma_0 = \mathrm{id}$, $\sigma_1 = d^+$, $\sigma_2 = (dw)^+$, $\sigma_3 = (d+dw)^+$, $\sigma_4 = (1+d+(1+d)w)^\bullet$, $\sigma_5 = \sigma_4 1^+$, $\sigma_6 = (1+d)^+ \imath 1^+ d^\bullet$, $\sigma_7 = \sigma_6 w^+$, $\sigma_8 = \sigma_6 1^+$, $\sigma_9 = \sigma_6 (1+w)^+$, and $\sigma_i = \sigma_{i-6}\sigma_2$ for $i = 10, \ldots, 15$. Then $\Sigma = \{\sigma_i \mid 0 \leqslant i \leqslant 15\}$ is a* 5-PD*-set for $I = \{0,1,w,1+w\}$, and $\mathscr{B}(I)$ is an independent set of the projective space V^*/K^*. The lower bound on the size for a* 5-PD*-set for I is* 10.

Proof. Put $A_i = \sigma_i^{-1}(I)$, and $D = A_0 \cup A_1$, $U = A_2 \cup A_3$. Note that $\sigma_2(U) = D$ and $\overline{L} = A_0 \dot\cup A_1 \dot\cup A_2 \dot\cup A_3 \dot\cup \{\infty\}$ is a disjoint union. Then

$$A_0 = \{0,1,w,1+w\}, \quad A_1 = \{d, 1+d, d+w, 1+d+w\},$$

$$A_4 = \{0,w,d+w,d\}, \quad A_5 = \{1, 1+w, 1+d+w, 1+d\},$$

$$A_6 = \{d,1,1+w,w\}, \quad A_7 = \{d+w, 1+w, 1, 0\},$$

$$A_8 = \{1+d, 0, w, 1+w\}, \quad A_9 = \{1+d+w, w, 0, 1\}.$$

Note that $A_i \subset D$ for $i = 4, \ldots, 9$, and $A_4 \cap A_5 = \emptyset$, $A_4 \cup A_5 = D$.

Let $B \subset \overline{L}$ with $|B| = 5$ and assume $B \cap A_i \neq \emptyset$ for $i = 0, 1, 2, 3$. Then two cases occur: $|D \cap B| = 2$ or $|U \cap B| = 2$.

Case 1: $|D \cap B| = 2$. Let $\{b_0, b_1\} = D \cap B$ with $b_0 \in A_0$, $b_1 \in A_1$. Assume $B \cap A_i \neq \emptyset$ for $i = 4, 5, 6, 8$.

Case 1.1: $b_0 \in A_4 \cap A_0 = \{0, w\}$. Then $b_0 \notin A_5$. Hence $b_1 \in A_5 \cap A_1 = \{1+d, 1+d+w\}$ because of $A_5 \cap B \neq \emptyset$, $A_5 \subset D$, thus $b_1 \notin A_6$, A_7, and $b_0 \notin A_6$ or $b_0 \notin A_7$. Hence b_0, $b_1 \notin A_6$ or b_0, $b_1 \notin A_7$. So, for $j = 6$ or $j = 7$ we have $B \cap A_j = \emptyset$, thus $\sigma_j(B) \cap I = \emptyset$.

Case 1.2: $b_0 \in A_5 \cap A_0 = \{1, 1 + w\}$. Then $b_0 \notin A_4$. Hence $b_1 \in A_4 \cap A_1 = \{d, d + w\}$, thus $b_1 \notin A_8$, A_9, and $b_0 \notin A_8$ or $b_0 \notin A_9$. Hence for $j = 8$ or $j = 9$ we have $\sigma_j(B) \cap I = \emptyset$.

Case 2: $|U \cap B| = 2$. Then $2 = |\sigma_2(U \cap B)| = |D \cap \sigma_2(B)|$. By Case 1 there is an $i \in \{4, \ldots, 9\}$ with $\emptyset = \sigma_i\sigma_2(B) \cap I = \sigma_{i+6}(B) \cap I$.

The image of I under $\mathscr{B}$ is

$$\mathscr{B}(I) = \{K^*(0, 0, 1), K^*(1, 1, 1), K^*(d, w, 1), K^*(d, 1 + w, 1\},$$

where, as before, the middle component is in L. Since $(0, 0, 1)$, $(1, 1, 1)$, $(d, w, 1)$, $(d, 1 + w, 1)$ are linearly independent, $\mathscr{B}(I)$ is an independent set of V^*/K^*.

The lower bound on the size of a PD-set is here

$$\left\lceil \frac{17}{13} \left\lceil \frac{16}{12} \left\lceil \frac{15}{11} \left\lceil \frac{14}{10} \left\lceil \frac{13}{9} \right\rceil \right\rceil \right\rceil \right\rceil \right\rceil = 10. \quad \square$$

Let $\mathbb{D} = K + K\varepsilon$ be the algebra of the dual numbers over K. For $y \in K$ we identify the point $\mathbb{D}^*(1, y\varepsilon)$ with (∞, y). For $y = 0$ we have $\infty = (\infty, 0)$. For $b \in K$ let b^{++} denote the permutation of the projective line $\mathbb{P}(L)$ induced by the matrix $\left(\begin{smallmatrix} 1 & b\varepsilon \\ 0 & 1 \end{smallmatrix}\right)$.

Proposition 8. *Let $K = \mathrm{GF}(3)$ and $\mathbb{D} = K + K\varepsilon$ the dual numbers over K. Then*

$$\Sigma = \{\mathrm{id}, 2^\bullet \imath (1 + \varepsilon)^+, 2^\bullet 2^+ \imath 2^+ \imath 2^\bullet (2 + \varepsilon)^+ 2^{++}\}$$

is a 2-PD-*set for $I = \{0, 1, 2, \varepsilon\}$. $\mathscr{B}(I)$ is an independent set of the projective space V^*/K^*. The lower bound for a* 2-PD-*set for I is* 3.

Proof. Put $\sigma_0 = \mathrm{id}$, $\sigma_1 = 2^\bullet \imath (1 + \varepsilon)^+$, $\sigma_2 = 2^\bullet 2^+ \imath 2^+ \imath 2^\bullet (2 + \varepsilon)^+ 2^{++}$ and $A_i = \sigma_i^{-1}(I)$. Then $A_0 = I$ and $A_1 = \{(\infty, 0), 1 + 2\varepsilon, 2\varepsilon, (\infty, 2)\}$, $A_2 = \{2 + \varepsilon, 1 + \varepsilon, (\infty, 1), 2 + 2\varepsilon\}$.

Let $B \subset \mathbb{P}(L)$ with $|B| = 2$. Since $\mathbb{P}(L) = A_0 \dot\cup A_1 \dot\cup A_2$ is a disjoint union there is an $i \in \{0, 1, 2\}$ with $B \cap A_i = \emptyset$; hence $\sigma_i(B) \subset \mathbb{P}(L) \backslash I$.

As in the proof of Proposition 6 the image $\mathscr{B}(I)$ is an independent set. Here we have $|\Sigma| \geqslant \left\lceil \frac{12}{8} \left\lceil \frac{11}{7} \right\rceil \right\rceil = 3$. $\square$

Remark. The mappings σ_1 and σ_2 are induced by the matrices

$$\begin{pmatrix} 0 & 1 \\ 2 & 1 + \varepsilon \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 + \varepsilon & 1 \\ 2 + 2\varepsilon & \varepsilon \end{pmatrix}.$$

Lemma 2. *Let* $M = \{x_1, x_1', x_2, x_2', y_1, y_1', y_2, y_2'\}$ *be a set of eight elements, and let*

$$A_0 = \{x_1, x_1', x_2, x_2'\}, \quad A_1 = \{y_1, y_1', y_2, y_2'\}, \quad A_2 = \{x_1, x_1', y_1, y_1'\},$$

$$A_3 = \{x_2, x_2', y_2, y_2'\}, \quad A_4 = \{x_1, x_1', y_2, y_2'\}, \quad A_5 = \{x_2, x_2', y_1, y_1'\}.$$

For every 2*-set* $B = \{b_0, b_1\} \subset M$ *there exists an* $i \in \{0, 1, 2, 3, 4, 5\}$ *with* $A_i \cap B = \emptyset$.

Proof. Let $B \cap A_j \neq \emptyset$ for $j = 0, 1, 2, 3$. Since $M = A_0 \dot\cup A_1$ is a disjoint union we may assume $b_0 \in A_0$ and $b_1 \in A_1$.

Case 1: $b_0 \in A_2$. Then $b_0 \in A_0 \cap A_2 = \{x_1, x_1'\}$, and hence $b_0 \notin A_3, A_5$. Also, $b_1 \in A_3$ because of $A_2 \cap A_3 = \emptyset$, hence $b_1 \in A_1 \cap A_3 = \{y_2, y_2'\}$, and thus $b_1 \notin A_5$. Therefore $A_5 \cap B = \emptyset$.

Case 2: $b_0 \in A_3$. By analogy with Case 1 we have $b_0 \notin A_2, A_4$ and $b_1 \in A_1 \cap A_2 = \{y_1, y_1'\}$, hence $b_1 \notin A_4$ and thus $A_4 \cap B = \emptyset$. □

Let $\mathbb{A} = K \times K$ be the algebra of the anormal complex numbers over K. For $x, y \in K$ we identify the point $\mathbb{A}^*((x, 1), (1, 0))$ with (x, ∞), and the point $\mathbb{A}^*((1, y), (0, 1))$ with (∞, y). Also, put $(\infty, \infty) = \infty$. With these notations the projective line $\mathbb{P}(\mathbb{A}) = \overline{K} \times \overline{K}$ where $\overline{K} = K \cup \{\infty\}$ is the projective line over K, and the mapping

$$\mathscr{B} : (x, y) \mapsto \begin{cases} K^*(xy, x, y, 1) & \text{for } x, y \in K, \\ K^*(x, 0, 1, 0) & \text{for } x \in K, \quad y = \infty, \\ K^*(y, 1, 0, 0) & \text{for } y \in K, \quad x = \infty, \\ K^*(1, 0, 0, 0) & \text{for } x = y = \infty. \end{cases}$$

For every bijection $\alpha : \overline{K} \to \overline{K}$, let

$$\acute{\alpha} : \overline{K} \times \overline{K} \to \overline{K} \times \overline{K}, \quad (x, y) \mapsto (\alpha(x), y),$$

$$\grave{\alpha} : \overline{K} \times \overline{K} \to \overline{K} \times \overline{K}, \quad (x, y) \mapsto (x, \alpha(y)),$$

$$\hat{\alpha} = \acute{\alpha} \circ \grave{\alpha}.$$

For every mapping $\alpha \in \mathrm{PGL}(2, K)$ the bijections $\acute{\alpha}$ and $\grave{\alpha}$ are in $\mathbb{M}_K(\mathbb{A}, K)$ (cf. [12]).

Let $I = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$. Then the subset

$$\mathscr{B}(I) = \{K^*(0, 0, 0, 1), K^*(0, 1, 0, 1), K^*(0, 0, 1, 1), K^*(1, 1, 1, 1)\}$$

of the hyperbolic quadric $\mathscr{B}(\overline{K} \times \overline{K})$ is an independent set of $\mathrm{PG}(3, K)$.

Proposition 9. *Let* $K = \mathrm{GF}(3)$ *and* $\mathbb{A} = K \times K$ *the algebra of the anormal complex numbers over* K. *Let* $\alpha = 2^\bullet\imath$, $\beta = 2^\bullet$, $\gamma = 2^+$, $\delta = \imath 1^+ \in \mathrm{PGL}(2, K)$. *Then*

$$\Sigma = \{\mathrm{id}, \acute{\alpha}, \grave{\alpha}, \hat{\alpha}, \acute{\beta}, \acute{\imath}, \acute{\gamma}, \acute{\delta}\}$$

is a 4*-PD-set for* $I = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$. *The lower bound on the size for a* 4*-PD-set for* I *is* 7.

Proof. Put $\sigma_0 = \mathrm{id}$, $\sigma_1 = \acute{\alpha}$, $\sigma_2 = \grave{\alpha}$, $\sigma_3 = \hat{\alpha}$, $\sigma_4 = \acute{\beta}$, $\sigma_5 = \acute{\imath}$, $\sigma_6 = \acute{\gamma}$, $\sigma_7 = \acute{\delta}$ and $A_i = \sigma_i^{-1}(I)$. Then

$$A_0 = \{(0,0),(1,0),(0,1),(1,1)\}, \quad A_1 = \{(\infty,0),(2,0),(\infty,1),(2,1)\},$$

$$A_2 = \{(0,\infty),(0,2),(1,\infty),(1,2)\}, \quad A_3 = \{(\infty,\infty),(2,2),(2,\infty),(\infty,2)\},$$

$$A_4 = \{(0,0),(2,0),(0,1),(2,1)\}, \quad A_5 = \{(\infty,0),(1,0),(\infty,1),(1,1)\},$$

$$A_6 = \{(1,0),(2,0),(1,1),(2,1)\}, \quad A_7 = \{(0,0),(0,1),(\infty,0),(\infty,1)\}.$$

Let $B = \{b_0, b_1, b_2, b_3\} \subset \overline{K} \times \overline{K}$. Let $B \cap A_i \neq \emptyset$ for $i = 0, 1, 2, 3, 4, 5$. Since $\overline{K} \times \overline{K} = \cup_{i=0}^{3} A_i$ is a disjoint union we may assume $b_i \in A_i$ for $i = 0, 1, 2, 3$. We have $A_4 \cup A_5 = A_0 \cup A_1 \ni b_0, b_1$. Also, A_6, $A_7 \subset A_0 \cup A_1$ and $(A_0 \cup A_1) \cap B = \{b_0, b_1\}$. By Lemma 2, $A_6 \cap B = \emptyset$ or $A_7 \cap B = \emptyset$, hence $\sigma_6(B) \cap I = \emptyset$ or $\sigma_7(B) \cap I = \emptyset$.

Again by Theorem 3, the lower bound on the size of a PD-set is $\lceil \frac{16}{12} \lceil \frac{15}{11} \lceil \frac{14}{10} \lceil \frac{13}{9} \rceil \rceil \rceil \rceil = 7$. □

Proposition 10. *Let $K = \mathrm{GF}(4) = \mathbb{Z}_2(d)$ with $d^2 = d + 1$ and $\mathbb{A} = K \times K$ the algebra of the anormal complex numbers over K. Let $\alpha = d^+$, $\beta = (d+1)^\bullet$, $\gamma = d^\bullet$, $\delta = 1^+ \in \mathrm{PGL}(2, K)$. Put*

$$\sigma_0 = \mathrm{id}, \quad \sigma_1 = \grave{\alpha}, \quad \sigma_2 = \acute{\alpha}, \quad \sigma_3 = \hat{\alpha}, \quad \sigma_4 = \grave{\beta}, \quad \sigma_5 = \grave{\beta}\grave{\delta}, \quad \sigma_6 = \grave{\gamma},$$

$$\sigma_7 = \grave{\gamma}\grave{\delta}, \quad \sigma_8 = \acute{\alpha}\grave{\beta}, \quad \sigma_9 = \acute{\alpha}\grave{\beta}\grave{\delta}, \quad \sigma_{10} = \acute{\alpha}\grave{\gamma}, \quad \sigma_{11} = \acute{\alpha}\grave{\gamma}\grave{\delta}, \quad \sigma_{12} = \grave{\imath},$$

$$\sigma_{13} = \grave{\imath}\grave{\delta}, \quad \sigma_{14} = \grave{\imath}\grave{\alpha}, \quad \sigma_{15} = \grave{\imath}\grave{\beta}, \quad \sigma_{16} = \acute{\alpha}\grave{\imath}, \quad \sigma_{17} = \acute{\alpha}\grave{\imath}\grave{\delta},$$

$$\sigma_{18} = \acute{\alpha}\grave{\imath}\grave{\alpha}, \quad \sigma_{19} = \acute{\alpha}\grave{\imath}\grave{\beta}.$$

Then the following hold:

(1) $\Sigma_1 = \{\sigma_i \mid 0 \leqslant i \leqslant 11\}$ *is a* 5-PD-*set for* $I = \{(0,0),(1,0),(0,1),(1,1)\}$. *The lower bound on the size for a* 5-PD-*set for I is* 6.
(2) $\Sigma_2 = \{\sigma_i \mid 0 \leqslant i \leqslant 19\}$ *is a* 7-PD-*set for I. The lower bound on the size for a* 7-PD-*set for I is* 11.
(3) Σ_1 *is a* 5-PD-*set of* $K \times K$ *for I. The lower bound on the size for a* 5-PD-*set for I is* 10.

Proof. Put $A_i = \sigma_i^{-1}(I)$, and $L = A_0 \cup A_1$, $R = A_2 \cup A_3$. Then,

$$A_0 = \{(0,0),(1,0),(0,1),(1,1)\},$$

$$A_1 = \{(0,d),(1,d),(0,d+1),(1,d+1)\},$$

$$A_2 = \{(d,0),(d+1,0),(d,1),(d+1,1)\},$$

$$A_3 = \{(d,d),(d+1,d),(d,d+1),(d+1,d+1)\},$$

$$A_4 = \{(0,0),(1,0),(0,d),(1,d)\},$$

$$A_5 = \{(0,1),(1,1),(0,d+1),(1,d+1)\},$$

$$A_6 = \{(0,0), (1,0), (0,d+1), (1,d+1)\},$$

$$A_7 = \{(0,1), (1,1), (0,d), (1,d)\},$$

$$A_8 = \{(d,0), (d+1,0), (d,d), (d+1,d)\},$$

$$A_9 = \{(d,1), (d+1,1), (d,d+1), (d+1,d+1)\},$$

$$A_{10} = \{(d,0), (d+1,0), (d,d+1), (d+1,d+1)\},$$

$$A_{11} = \{(d,1), (d+1,1), (d,d), (d+1,d)\},$$

$$A_{12} = \{(0,\infty), (1,\infty), (0,1), (1,1)\},$$

$$A_{13} = \{(0,\infty), (1,\infty), (0,0), (1,0)\},$$

$$A_{14} = \{(0,\infty), (1,\infty), (0,d+1), (1,d+1)\},$$

$$A_{15} = \{(0,\infty), (1,\infty), (0,d), (1,d)\},$$

$$A_{16} = \{(d,\infty), (d+1,\infty), (d,1), (d+1,1)\},$$

$$A_{17} = \{(d,\infty), (d+1,\infty,), (d,0), (d+1,0)\},$$

$$A_{18} = \{(d,\infty), (d+1,\infty), (d,d+1), (d+1,d+1)\},$$

$$A_{19} = \{(d,\infty), (d+1,\infty), (d,d), (d+1,d)\},$$

where $A_j \subset L$ for $j = 4, 5, 6, 7$, $A_k \subset R$ for $k = 8, 9, 10, 11$ and $A_j \subset L_\infty = L \cup \{(0,\infty), (1,\infty)\}$ for $j = 12, 13, 14, 15$ and $A_k \subset R_\infty = R \cup \{(d,\infty), (d+1,\infty)\}$ for $k = 16, 17, 18, 19$.

(1) Let $B = \{b_0, b_1, b_2, b_3, b_4\} \subset \overline{K} \times \overline{K}$ and assume $B \cap A_j \neq \emptyset$ for $j = 0, 1, 2, 3$. Since $A_0 \dot\cup A_1 \dot\cup A_2 \dot\cup A_3$ is a disjoint union we may assume $b_j \in A_j$ for $j = 0, 1, 2, 3$, hence $b_0, b_1 \in L$ and $b_2, b_3 \in R$, and thus $|B \cap L| = 2$ or $|B \cap R| = 2$. Without loss of generality we may assume $|B \cap L| = 2$. By Lemma 2 there exists an $i \in \{4, 5, 6, 7\}$ with $b_0, b_1 \notin A_i$. Because of $B \cap L = \{b_0, b_1\}$ and $A_i \subset L$ we have $A_i \cap B = \emptyset$, hence $\sigma_i(B) \cap I = \emptyset$.

The lower bound on the size of a PD-set is here

$$\left\lceil \frac{25}{21} \left\lceil \frac{24}{20} \left\lceil \frac{23}{19} \left\lceil \frac{22}{18} \left\lceil \frac{21}{17} \right\rceil \right\rceil \right\rceil \right\rceil \right\rceil = 6.$$

(2) Let $B \subset \overline{K} \times \overline{K}$ with $|B| = 7$. If $|B \cap L| \leqslant 2$ or $|B \cap R| \leqslant 2$ then there exists a $\sigma \in \Sigma_1$ with $\sigma(B) \cap I = \emptyset$. So we may assume $|B \cap L|, |B \cap R| \geqslant 3$. Then $|B \cap L_\infty| = 3$ or $|B \cap R_\infty| = 3$. Without loss of generality we may assume $|B \cap L_\infty| = 3$. Then $(0,\infty)$, $(1,\infty) \notin B$ and there exists $y \in K$ with $(0, y), (1, y) \notin B$. Inspecting the sets $A_{12}, A_{13}, A_{14}, A_{15}$ we see that there is $j \in \{12, 13, 14, 15\}$ with $(0, y), (1, y) \in A_j$; hence $B \cap A_j = \emptyset$, thus $\sigma_j(B) \cap I = \emptyset$.

Here the lower bound is

$$\left\lceil \frac{25}{21} \left\lceil \frac{24}{20} \left\lceil \frac{23}{19} \left\lceil \frac{22}{18} \left\lceil \frac{21}{17} \left\lceil \frac{20}{16} \left\lceil \frac{19}{15} \right\rceil \right\rceil \right\rceil \right\rceil \right\rceil \right\rceil \right\rceil = 11.$$

(3) follows by (1) from the fact that $\sigma(K \times K) = K \times K$ for all $\sigma \in \Sigma_1$. The bound is

$$\left\lceil \frac{16}{12} \left\lceil \frac{15}{11} \left\lceil \frac{14}{10} \left\lceil \frac{13}{9} \left\lceil \frac{12}{8} \right\rceil \right\rceil \right\rceil \right\rceil \right\rceil = 10. \qquad \square$$

The next result follows from Proposition 2, 5, 6, 8, 9 and Lemma 1.

Proposition 11. *Let Q be a quadric in* PG$(3, 3)$ *and let* $\mathbf{v}$ *be a vector representation.*

(1) *If Q is elliptic, then $C(\mathbf{v}, Q)$ is a* 2*-error-correcting* $[10, 4, 6]_3$*-code admitting a* PD*-set S of minimum size* 4.
(2) *If Q is a cone with vertex s, then $C(\mathbf{v}, Q\backslash\{s\})$ is a* 2*-error-correcting* $[12, 4, 6]_3$*-code admitting a* PD*-set S of minimum size* 3.
(3) *If Q is hyperbolic, then $C(\mathbf{v}, Q)$ is a* 4*-error-correcting* $[16, 4, 9]_3$*-code admitting a* PD*-set S of size* 8.

Propositions 2, 7, and Lemma 1 imply the following result.

Proposition 12. *Let Q be an elliptic quadric in* PG$(3, 4)$ *and let* $\mathbf{v}$ *be a vector representation. Then $C(\mathbf{v}, Q)$ is a* 5*-error-correcting* $[17, 4, 12]_4$*-code admitting a* PD*-set S of size* 16.

Proposition 13. *Let Q be a hyperbolic quadric in* PG$(3, 4)$ *and let* $\mathbf{v}$ *be a vector representation. Then*

(1) *$C(\mathbf{v}, Q)$ is a* $[25, 4, 16]_4$*-code admitting a* PD*-set S of size* 20.
(2) *Let $p \in Q$ and $[p]$ the union of the two generators on Q passing through p. Then $C(\mathbf{v}, Q\backslash[p])$ is a* $[16, 4, 9]_4$*-code admitting a* PD*-set S of size* 12.

Proof. (1) This follows from Proposition 2, 10 and Lemma 1.
(2) Put $A = Q\backslash[p]$. Note first that

$$\max\{|A \cap H| \, | \, H \in \mathfrak{H}\} = |A| - (2q + 1) = q(q - 2) + 1 = 9.$$

Hence $C(\mathbf{v}, A)$ is a 4-error but not 5-error-correcting code. Since the automorphism group of Q operates transitively on Q we may assume $p = \mathscr{B}(\infty, \infty)$. The assertion now follows by (3) from Proposition 10. $\square$

Remark. The lower bound on the size of the codes in Proposition 13 is 11 and 7, respectively.

4. Automorphisms of the celtic variety

Let K be a commutative field and K^5 the five-dimensional vector space over K. Let $\overline{K} = K \cup \{\infty\}$ denote the projective line over K. The mapping

$$p : \begin{cases} \overline{K} \times \overline{K} \to K^{5*}/K^*, \\ (s,u) \mapsto \begin{cases} K^*(us, u, s, 1, s^2) & \text{for } s, u \in K, \\ K^*(u, 0, 0, 0, 1) & \text{for } s = \infty, \quad u \in K, \\ K^*(s, 1, 0, 0, 0) & \text{for } s \in K, \quad u = \infty, \\ K^*(1, 0, 0, 0, 0) & \text{for } s = \infty, \quad u = \infty \end{cases} \end{cases}$$

is injective.

The image $P = p(\overline{K} \times \overline{K})$ is the ruled rational normal variety of order 3 in the four-dimensional projective space PG(4, K) (cf. [2], Ch. 13,7.,8.,9. and [11]). The line $L = p(\overline{K} \times \{\infty\})$ and the conic $C = p(\overline{K} \times \{0\})$ are called the minimum-order directrix and the maximum-order directrix. The surface P can be generated by the projectivity that maps any point $l_s = p(s, \infty)$ of L to the point $c_s = p(s, 0)$ of C and is ruled by the generators $G_s = p(\{s\} \times \overline{K})$ joining corresponding points. We call the *celtic variety*.

Lemma 3. *Every automorphism $\alpha \in$ Aut P fixes the line-directrix L and maps every generator G_s to a generator $G_{s'}$.*

Proof. It is enough to note that L is the unique line on P intersecting the generators and that there are no other lines contained in P than L and the generators ([2,11]). □

For $m, b, c \in K$, $m \neq 0$, let $[m, b]$, $[m, b, c]$, ι denote the projective collineations of PG(4, K) induced by the respective matrices

$$\begin{pmatrix} m & 0 & 0 & 0 & 0 \\ b & 1 & 0 & 0 & 0 \\ 0 & 0 & m & 0 & 2mb \\ 0 & 0 & b & 1 & b^2 \\ 0 & 0 & 0 & 0 & m^2 \end{pmatrix}, \quad \begin{pmatrix} m & 0 & 0 & 0 & 0 \\ 0 & m & 0 & 0 & 0 \\ b & c & 1 & 0 & 0 \\ 0 & b & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Proposition 14. (1) $\mathscr{A} = \{[m, b] \mid m, b \in K, m \neq 0\}$ *is a subgroup of* Aut P.
(2) $\iota \in$ Aut P.
(3) *For every $\alpha \in \mathscr{A} \cup \{\iota\}$ we have $\alpha(L) = L$ and $\alpha(C) = C$.*
(4) $\mathscr{N} = \{\nu \in \text{Aut } P \mid \forall s \in \overline{K} : \nu(G_s) = G_s\}$ *is a normal subgroup of* Aut P. *For every $\alpha \in \mathscr{N}$, $L \subset$ Fix α.*
(5) $\mathscr{N}' = \{[m, b, c] \mid m, b, c \in K m \neq 0\}$ *is a subgroup of $\mathscr{N}$.*

Proof. (1) For $[m, b], [m', b'] \in \mathscr{A}$ we have $[m', b'] \circ [m, b] = [mm', bm' + b']$. Hence the affine group Aff(K), i.e. the group of the bijections : $K \to K$, $x \mapsto xm + b$ ($m, b \in K$, $m \neq 0$), is isomorphic to $\mathscr{A}$. Thus $\mathscr{A}$ is a subgroup of the automorphism group of PG(4, K). For $[m, b] \in \mathscr{A}$ and $p(s, u) \in P$ we have

$$[m, b](p(s, u)) = \begin{cases} p(sm + b, u) & \text{for } s \in K, \quad u \in \overline{K} \\ p(\infty, um^{-1}) & \text{for } s = \infty, \quad u \in \overline{K} \end{cases}.$$

Hence, $[m, b](P) \subset P$ and $[m, b]^{-1}(P) = [m^{-1}, -bm^{-1}](P) \subset P$, thus $[m, b](P) = P$.

(2) We have $\iota^2 = \mathrm{id}$ and

$$\iota(p(s,u)) = \begin{cases} p(s^{-1}, us^{-1}) & \text{for } s, u \in K, \quad s \neq 0, \\ p(\infty, u) & \text{for } s = 0, \quad u \in \overline{K}, \\ p(0, u) & \text{for } s = \infty, \quad u \in \overline{K}, \\ p(s^{-1}, \infty) & \text{for } s \neq 0, \infty, \quad u = \infty; \end{cases}$$

hence $\iota(P) = P$.

(3) This follows from (1) and (2).

(4) Clearly, $\mathcal{N}$ is a subgroup of $\mathrm{Aut}\, P$. Let $\alpha \in \mathrm{Aut}\, P$ and $\nu \in \mathcal{N}$. By Lemma 3, $\alpha(L) = L = \nu(L)$, hence $L \subset \mathrm{Fix}\, \nu$ and, $L \subset \mathrm{Fix}\, \alpha\nu\alpha^{-1}$, and thus $\alpha\nu\alpha^{-1} \in \mathcal{N}$.

(5) Since $[m', b', c'] \circ [m, b, c] = [mm', bm' + b', cm' + c']$ and $[m, b, c]^{-1} = [m^{-1}, -bm^{-1}, -cm^{-1}]$ the set $\mathcal{N}'$ is a subgroup of the automorphism group of $\mathrm{PG}(4, K)$. For $[m, b, c] \in \mathcal{N}'$ and $p(s, u) \in P$ we have

$$[m, b, c](p(s,u)) = \begin{cases} p(s, um + sc + b) & \text{for } s, u \in K, \\ p(\infty, um + c) & \text{for } s = \infty, \quad u \in K, \\ p(s, \infty) & \text{for } s \in K, \quad u = \infty, \\ p(\infty, \infty) & \text{for } s = u = \infty; \end{cases}$$

hence $[m, b, c](G_s) = G_s$, and $[m, b, c](P) = P$. □

Remark. By Proposition 14 the subgroup $\Gamma = \{\alpha \in \mathrm{Aut}\, P \mid \alpha(C) = C\}$ is isomorphic to $\mathrm{PGL}(2, K)$. The group $\mathrm{Aut}\, P$ can be written as faithful product of $\mathcal{N}$ and $\mathrm{PGL}(2, K)$ if we identify the elements of Γ with those of $\mathrm{PGL}(2, K)$. It can be proved that $\mathcal{N}' = \mathcal{N}$.

Now, let $K = \mathrm{GF}(q)$. Then $|P| = (q+1)^2$. Let $H \in \mathfrak{H}$ be a hyperplane. The intersection $P \cap H$ is the union of a generator and a conic or the union of two generators and L or the union of one generator and L or L or a cubic curve (cf. [10, Lemma 11]). Hence $\max\{|P \cap H| | H \in \mathfrak{H}\} = 3q + 1$. Since P generates $\mathrm{PG}(4, q)$ we obtain the first two parts of the next result.

Proposition 15. *Let* $\mathbf{v}$ *be a vector representation of* $\mathrm{PG}(4, q)$.

(1) $C(\mathbf{v}, P)$ *is a* $[(q+1)^2, 5, q(q-1)]_q$*-linear code.*

(2) $C(\mathbf{v}, P \backslash L)$ *is a* $[q(q+1), 5, q(q-1)]_q$*-linear code.*

(3) *Let* $q \geqslant 4$ *and* $I \subset P$ *an independent set of* $\mathrm{PG}(4, q)$. *If* $I \cap L \neq \emptyset$, *then there is no* PD*-set for* I.

Proof. (3) For $q \geqslant 4$ the inequality $(q+1)^2 > 5q + 2$ holds; hence

$$\left\lfloor \frac{q(q+1) - 1}{2} \right\rfloor \geqslant q + 1 = |L|.$$

Lemma 3 and Proposition 5 now yield the assertion. □

Proposition 16. *Let P be the celtic variety in* PG(4, 3) *and let*

$$I' = \{p(0,1),\ p(0,2),\ p(1,\infty),\ p(2,1),\ p(\infty,0)\}.$$

Then $\Sigma = \{\mathrm{id},\ \imath[1,1],\ [1,1]\imath[1,1][1,1,0]\}$ *is a* 2-PD-*set for* I'. *The lower bound for a* 2-PD-*set of* P *is* 3.

Proof. Put $\sigma_0 = \mathrm{id}$, $\sigma_1 = \imath[1,1]$, $\sigma_2 = [1,1]\imath[1,1][1,1,0]$ and $A_i = \sigma_i^{-1}(I)$. Then $A_0 = I$ and

$$A_1 = \{p(\infty,1),\ p(\infty,2),\ p(0,\infty),\ p(1,2),\ p(2,0)\},$$

$$A_2 = \{p(1,1),\ p(1,0),\ p(\infty,\infty),\ p(0,0),\ p(2,2)\}.$$

Let $B \subset P$ with $|B| = 2$. Since $A_0 \cap A_1 = \emptyset$, $A_0 \cap A_2 = \emptyset$, $A_1 \cap A_2 = \emptyset$, there is an $i \in \{0,1,2\}$ with $B \cap A_i = \emptyset$, hence $\sigma_i(B) \cap I = \emptyset$. □

Remarks. 1. The mappings σ_1 and σ_2 are induced by the matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

2. Note that I' is an independent set of PG(3, K) if char $K \neq 2$.

3. Let $q = 3$, $I \subset P$ an independent set of PG(4, 3) with $|I| = 5$ and $|I \cap L| = 2$, and let Σ be a 2-PD-set for I. Then $\mathrm{Rest}_L \Sigma = \{\sigma|_L \mid \sigma \in \Sigma\}$ is a 2-PD-set for $I \cap L$, hence by Theorem 1 we have

$$|\mathrm{Rest}_L\ \Sigma| \geqslant \left\lceil \frac{4}{2} \left\lceil \frac{3}{1} \right\rceil \right\rceil = 6,$$

and thus $|\Sigma| \geqslant 6$. This says that the size of a PD-set depends on the choice of the information set I. The problem to determine a smallest PD-set of a code includes the problem to determine a suitable set I of information positions (cf. also Proposition 15).

Propositions 15 and 16 give the following result.

Proposition 17. *Let P be the celtic variety in* PG(4, 3) *and let* $\mathbf{v}$ *be a vector representation. Then* $C(\mathbf{v}, P)$ *is a* 2-*error-correcting* $[16, 5, 6]_3$-*code admitting a* PD-*set S of minimum size* 3.

The set $I = p(\{(0,0),\ (0,1),\ (1,0),\ (1,1),\ (\infty,0)\})$ is an independent set of PG(4, K).

Proposition 18. *Let P be the celtic variety in* PG(4, 4). *Put*

$$\sigma_0 = \mathrm{id}, \quad \sigma_1 = [1,d,1], \quad \sigma_2 = [1,d][1,0,d], \quad \sigma_3 = \sigma_1\sigma_2,$$

$$\sigma_4 = [d+1,0,0], \quad \sigma_5 = [d+1,d,0], \quad \sigma_6 = [d,0,0], \quad \sigma_7 = [d,d,0],$$

$$\sigma_8 = [1, 0, 1], \quad \sigma_9 = [1, d, 0], \quad \sigma_{10} = [1, 0, d], \quad \sigma_{11} = [1, 0, d+1],$$

$$\sigma_{12} = [1, d]\iota[1, d], \quad \sigma_{13} = \sigma_{12}[1, 1, 0], \quad \sigma_{14} = [d+1, 0, 1][1, d],$$

$$\sigma_{15} = [d+1, d, 1][1, d], \quad \sigma_{16} = [d, 0, 1][1, d][1, 0, 1],$$

$$\sigma_{17} = [d, d, 1][1, d][1, 0, 1], \quad \sigma_{18} = [1, d][1, 0, d+1],$$

$$\sigma_{19} = \sigma_2\sigma_9, \quad \sigma_{20} = \sigma_2\sigma_{10}, \quad \sigma_{21} = \sigma_2\sigma_{11}, \quad \sigma_{22} = \iota, \quad \sigma_{23} = \iota[1, 1, 0].$$

Then $\Sigma = \{\sigma_i \mid 0 \leqslant i \leqslant 23\}$ *is a* 5-PD*-set of* $P\backslash L$ *for I. The lower bound on the size of a* 5-PD*-set of* $P\backslash L$ *is* 10.

Proof. Again put $A_i = \sigma_i^{-1}(I)$. Since the mapping p is injective we identify $p(s, u)$ with (s, u). Then

$$A_1 = \{(0, d), (0, d+1), (1, d+1), (1, d), (\infty, 1)\}$$

$$A_2 = \{(d, d+1), (d, d), (1+d, 1), (1+d, 0), (\infty, d)\},$$

$$A_3 = \{(d, 1), (d, 0), (1+d, d), (1+d, 1+d), (\infty, 1+d)\},$$

$$A_4 = \{(0, 0), (0, d), (1, 0), (1, d), (\infty, 0)\},$$

$$A_5 = \{(0, 1+d), (0, 1), (1, 1+d), (1, 1), (\infty, 0)\},$$

$$A_6 = \{(0, 0), (0, d+1), (1, 0), (1, d+1), (\infty, 0)\},$$

$$A_7 = \{(0, 1), (0, d), (1, 1), (1, d), (\infty, 0)\},$$

$$A_8 = A_0' \cup \{(\infty, 1)\}, \quad \text{where } A_0' = A_0\backslash\{(\infty, 0)\},$$

$$A_9 = A_1' \cup \{(\infty, 0\}, \quad \text{where } A_1' = A_1\backslash\{(\infty, 1)\},$$

$$A_{10} = \{(0, 0), (0, 1), (1, d), (1, 1+d), (\infty, d)\},$$

$$A_{11} = \{(0, 0), (0, 1), (1, 1+d), (1, d), (\infty, 1+d)\},$$

$$A_{12} = \{(1, 0), (1, 1+d), (0, 0), (0, d), (d, 0)\},$$

$$A_{13} = \{(1, 1), (1, d), (0, 1), (0, 1+d), (d, 1)\},$$

Now, let $B = \{b_0, b_1, b_2, b_3, b_4\} \subset P\backslash L$ with $A_i \cap B \neq \emptyset$ for $i = 0, 1, 2, 3$. Since $P\backslash L = A_0 \dot\cup A_1 \dot\cup A_2 \dot\cup A_3$ is a disjoint union we may assume $b_i \in A_i$ for $i = 0, 1, 2, 3$. As $|B| = 5$ we have $|(A_0 \cup A_1) \cap B| = 2$ or $|(A_2 \cup A_3) \cap B| = 2$.

Case 1: $|(A_0 \cup A_1) \cap B| = 2$.

Case 1.1: $b_0 = (\infty, 0)$, $b_1 = (\infty, 1)$. Let $A_i \cap B \neq \emptyset$ for $i = 10, 11, 12$. Then (∞, d), $(\infty, 1+d)$, $(d, 0) \in B$ because of $B \cap (A_0' \cup A_1') = \emptyset$. Hence $(d, 1) \notin B$, and thus $A_{13} \cap B = \emptyset$.

Case 1.2: $b_0 = (\infty, 0)$, $b_1 \neq (\infty, 1)$. Then $b_1 \notin A_0' \cup \{(\infty, 1)\} = A_8$; hence $A_8 \cap B = \emptyset$.

Case 1.3: $b_0 \neq (\infty, 0)$, $b_1 \neq (\infty, 1)$. Let $A_4 \cap B \neq \emptyset$ and $A_5 \cap B \neq \emptyset$.

Case 1.3.1: $b_1 \in A_4 \cap A_1 = \{(0, d), (1, d)\}$. Then $b_1 \notin A_5, A_6$, hence $b_0 \in A_5 \cap A_0 = \{(0, 1), (1, 1), (\infty, 0)\}$, hence $b_0 \in \{(0, 1), (1, 1)\}$, thus $b_0 \notin A_6$, and therefore $A_6 \cap B = \emptyset$.

Case 1.3.2: $b_1 \in A_5 \cap A_1 = \{(0, 1+d), (1, 1+d)\}$. Then $b_1 \notin A_4, A_7$, hence $b_0 \in A_4 \cap A_0 = \{(0,0), (1,0), (\infty, 0)\}$, hence $b_0 \in \{(0,0), (1,0)\}$, thus $b_0 \notin A_7$, and therefore $A_7 \cap B = \emptyset$.

Case 2: $|(A_2 \cup A_3) \cap B| = 2$. This case can be treated as Case 1 using the sets A_{14} up to A_{23} instead of the sets A_4 up to A_{13}. □

Propositions 15 and 18 give the final result.

Proposition 19. *Let P be the celtic variety in* $\mathrm{PG}(4,4)$ *and let* $\mathbf{v}$ *be a vector representation. Then $C(\mathbf{v}, P\backslash L)$ is a five-error-correcting* $[20, 5, 12]_4$*-code admitting a* PD*-set S of size* 24.

References

[1] W. Benz, Vorlesungen über Geometrie der Algebren, Springer, Berlin-Heidelberg-New York, 1973.
[2] E. Bertini, Geometria proiettiva degli iperspazi, in: E. Spoerri (Ed.), Pisa, 1907.
[3] D.M. Gordon, Minimal permutations sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory IT-82 (1982) 541–543.
[4] W. Heise, P. Quattrocchi, Informations- und Codierungstheorie, 3. auflage edition, Springer, Berlin, 1995.
[5] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Clarendon Press, Oxford, 1991.
[6] H. Hotje, Einbettung gewisser Kettengeometrien in projektive Räume, J. Geom. 5 (1974) 85–94.
[7] H. Karzel, K. Sörensen, D. Windelberg, Einführung in die Geometrie, Vandenhoeck, Göttingen, 1973.
[8] V.S. Pless, W.C. Huffman (eds), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.
[9] M.A. Tsfasman, S.G. Vlăduţ, Algebraic-Geometric Codes, Mathematics and its Applications. vol. 58, Kluwer Academic Publishers, Dordrecht, 1991.
[10] R. Vincenti, On some classical varieties and codes, Rapp. Tecnico 2000/20 Dip-Mat. Inf. Univ. PG.
[11] R. Vincenti, Alcuni tipi di varietà, V_2^3 di $S_{4,q}$ e sottopiani di Baer, Suppl. BUMI, Algebra e Geometria 2 (1980) 31–44.
[12] H. Wefelscheid, Über die Automorphismengruppen von Hyperbelstrukturen, in: Beitr. Geom. Algebra, Proc. Symp. Duisburg 1976, 1977, pp. 337–343.